I05(12/28/2005) Com 1/4/7/2006

DEC 29 2005

PTO/SB/08a (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number.

OIPE DEC 29 2005 PATENT & TRADEMARK OFFICE

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	09/930,836
Filing Date	August 15, 2001
First Named Inventor	Paul C. Kocher
Group Art Unit	2132
Examiner Name	Justin T. Darrow
Attorney Docket No.r	44424162-8724

OTHER ITEMS – NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
JD		Posting on sci.crypt newsgroup, RIVEST, Ron, "Announce: Timing cryptanalysis of RSA, DH, DSS", 12-11-95, retrieved from internet 11-19-05, http://groups.google,com/group/sci.crypt/msg/79e75dc930adf?dmode=source&hl=en.	
JD		Posting on sci.crypt newsgroup, KOCHER, Paul C, "Announce: Timing cryptanalysis of RSA, DH, DSS", 12-11-95, retrieved from internet 11-19-05, http://groups.google,com/group/sci.crypt/msg/027dadba758893a5?dmode=source&hl=en.	
JD		Posting on sci.crypt newsgroup, WALTERS, Jim, "Announce: Timing cryptanalysis of RSA, DH, DSS", 12-11-95, retrieved from internet 11-19-05, http://groups.google,com/group/sci.crypt/msg/77b761989c18baea?dmode=source&hl=en.	
JD		Posting on sci.crypt newsgroup, KOCHER, Paul C, "Announce: Timing cryptanalysis of RSA, DH, DSS", 12-12-95, retrieved from internet 11-22-05, http://groups.google,com/group/sci.crypt/msg/769112d9a7a17488?dmode=source&hl=en.	
JD		Posting on sci.crypt newsgroup, RUBIN, Paul, "Announce: Timing cryptanalysis of RSA, DH, DSS", 12-12-95, retrieved from internet 11-22-05, http://groups.google,com/group/sci.crypt/msg/7c8fva520b1b5482?dmode=source&hl=en.	
JD		Posting on sci.crypt newsgroup, BROWN, Ralf, "Announce: Timing cryptanalysis of RSA, DH, DSS", 12-12-95, retrieved from internet 11-22-05, http://groups.google,com/group/sci.crypt/msg/417b42c49fe7cf53?dmode=source&hl=en.	
JD		Posting on sci.crypt newsgroup, STEWART, Bill, "Announce: Timing cryptanalysis of RSA, DH, DSS", 12-13-95, retrieved from internet 11-22-05, http://groups.google,com/group/sci.crypt/msg/7610aea60249ed48?dmode=source&hl=en.	
JD		Posting on sci.crypt newsgroup, Larry, "Announce: Timing cryptanalysis of RSA, DH, DSS", 12-15-95, retrieved from internet 11-22-05, http://groups.google,com/group/sci.crypt/msg/ced8289a35a32925?dmode=source&hl=en.	
JD		Posting on sci.crypt newsgroup, COSTA, Bob, "Re: Attacking machines on the Internet (re: Timing cryptanalysis of RSA, DH, DSS)", 12-16-95, retrieved from internet 11-22-05, http://groups.google,com/group/sci.crypt/msg/350820497cce62ba?dmode=source&hl=en.	

Examiner Signature	Justin Darrow	Date Considered	04/30/2006

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08a (08-03)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of info unless it contains a valid OMB control number.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 2 of 2

Complete if Known	
Application Number	09/930,836
Filing Date	August 15, 2001
First Named Inventor	Paul C. Kocher
Group Art Unit	2132
Examiner Name	Justin T. Darrow
Attorney Docket No.	44424162-8724

OTHER ITEMS – NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
JD		Posting on sci.crypt newsgroup, PERRY, Tom, "Announce: Timing cryptanalysis of RSA, DH, DSS", 12-17-95, retrieved from internet 11-22-05, http://groups.google,com/group/sci.crypt/msg/20e43912653f9bd0?dmode=source&hl=en.	
JD		Posting on sci.crypt newsgroup, BELL, Jim, "Spread-Spectrum computer clock?", 12-24-95, retrieved from internet 11-22-05, http://groups.google,com/group/sci.crypt/msg/485abca33cc29703?dmode=source&hl=en.	
JD		Posting on mail.cypherpunks, BRANDT, Eli, "Re: Timing Attacks", 12-11-95, retrieved from internet 12-7-05, http://groups.google.com/group/mail.cypherpunks/msg/fa276adeb23f2b83?dmode=source	
JD		Posting on mail.cypherpunks, Armadillo Remailer, "Re: Timing Attacks", 12-13-95, retrieved from internet 11-22-05, http://groups.google.com/group/mail.cypherpunks/msg/fedb10d2bcf3ff6f?dmod...	
JD		Posting on mail.cypherpunks, HOSELTON, Rick, "Re: Timing Cryptanalysis Attack", 12-14-95, retrieved from internet 11-22-05, http://groups.google.com/group/mail.cypherpunks/msg/470f2482c69f3212?dmo...	
JD		Declaration of Paul Kocher concerning the 1995 postings, KOCHER, Paul, 12-16-05	

Examiner Signature	Justin Darrow	Date Considered	04/30/2006

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.